Schneier on Security

Ransomware and the Internet of Things

As devastating as the latest widespread ransomware attacks have been, it's a problem with a solution. If your copy of Windows is relatively current and you've kept it updated, your laptop is immune. It's only older unpatched systems on your computer that are vulnerable.

Patching is how the computer industry maintains security in the face of rampant Internet insecurity. Microsoft, Apple and Google have teams of engineers who quickly write, test and distribute these patches, updates to the codes that fix vulnerabilities in software. Most people have set up their computers and phones to automatically apply these patches, and the whole thing works seamlessly. It isn't a perfect system, but it's the best we have.

But it is a system that's going to fail in the "Internet of things": everyday devices like smart speakers, household appliances, toys, lighting systems, even cars, that are connected to the web. Many of the embedded networked systems in these devices that will pervade our lives don't have engineering teams on hand to write patches and may well last far longer than the companies that are supposed to keep the software safe from criminals. Some of them don't even have the ability to be patched.

Fast forward five to 10 years, and the world is going to be filled with literally tens of billions of devices that hackers can attack. We're going to see ransomware against our cars. Our digital video recorders and web cameras will be taken over by botnets. The data that these devices collect about us will be stolen and used to commit fraud. And we're not going to be able to secure these devices.

Like every other instance of product safety, this problem will never be solved without considerable government involvement.

For years, I have been calling for more regulation to improve security in the face of this market failure. In the short term, the government can mandate that these devices have more secure default configurations and the ability to be patched. It can issue best-practice regulations for critical software and make software manufacturers liable for vulnerabilities. It'll be expensive, but it will go a long way toward improved security.

But it won't be enough to focus only on the devices, because these things are going to be around and on the Internet much longer than the two to three years we use our phones and computers before we upgrade them. I expect to keep my car for 15 years, and my refrigerator for at least 20 years. Cities will expect the networks they're putting in place to last at least that long. I don't want to replace my digital thermostat ever again. Nor, if I ever need one, do I want a surgeon to ever have to go back in to replace my computerized heart defibrillator in order to fix a software bug.

No amount of regulation can force companies to maintain old products, and it certainly can't prevent companies from going out of business. The future will contain billions of orphaned devices connected to the web that simply have no engineers able to patch them.

Imagine this: The company that made your Internet-enabled door lock is long out of business. You have no way to secure yourself against the ransomware attack on that lock. Your only option, other than paying, and paying again when it's reinfected, is to throw it away and buy a new one.

Ultimately, we will also need the network to block these attacks before they get to the devices, but there again the market will not fix the problem on its own. We need additional government intervention to mandate these sorts of solutions.

None of this is welcome news to a government that prides itself on minimal intervention and maximal market forces, but national security is often an exception to this rule. Last week's cyberattacks have laid bare some fundamental vulnerabilities in our computer infrastructure and serve as a harbinger. There's a lot of good research into robust solutions, but the economic incentives are all misaligned. As politically untenable as it is, we need government to step in to create the market forces that will get us out of this mess.

This essay previously appeared in the *New York Times*. Yes, I know I'm repeating myself.

EDITED TO ADD: A good cartoon.

Tags: cyberattack, Internet and society, Internet of things, ransomware, security engineering

Posted on May 25, 2017 at 6:15 AM • 43 Comments

Comments

Ido Sivan-Sevilla • May 25, 2017 6:58 AM

Liabilty shifting is key. I like the comparison to the product safety eco-system. There is too much money in the iot industry and I believe that iability shifting would not deter producers.

Bill Marrs • **May 25, 2017 7:27 AM**

White-hat hackers proactively gaining access to exposed iot devices and upgrading their security seems to have potential. Regulations and liability don't seem agile enough to respond to the crisis.

Jakub Narębski • **May 25, 2017 7:48 AM**

Some of security / safety related problems can be solved by market (UL = Underwriters Laboratory), some need to be solved by the government - when there is lack of transparency (FDA).

Thomas • **May 25, 2017 7:54 AM**

> [...] If your copy of $OPERATINGSYSTEM is relatively current and you've kept it updated, your laptop is immune.

This time... because the vendor had a chance to fix the vulnerability.
If someone weaponizes a 0-day then all the vendor patches in the world won't help.

> Microsoft, Apple and Google have teams of engineers who quickly write, test and distribute these patches,

Except for the Android patch system which is best described as the human centipede. By the time a patch has made it through Google, your phone vendor and your telco you've probably already upgraded to a new phone.

> Patching is how the computer industry maintains security in the face of rampant Internet insecurity.

To be fair, Internet insecurity is caused in large part by insecure software be those same vendors.

> Most people have set up their computers and phones to automatically apply these patches,

Most people no longer have a choice. Whether that's a good thing or not is debatable.

> Your only option, other than paying, and paying again when it's reinfected, is to throw it away and buy a new one.

Or, throw it away and buy an old one.
That's assuming some anti-terrorism law hasn't been passed that mandates government back-doors on people's front-doors.

> Ultimately, we will also need the network to block these attacks before they get to the devices,

If the internet becomes end-to-end encrypted by default then this might become quite challenging.

Etienne • **May 25, 2017 8:03 AM**

Microsoft pushed a Windows 10 update, and after 4 hours, it failed.

It said if it failed, to make an ISO disk and do it that way.

After 4 more hours that failed.

I assume this is why many non-professionals just stop updating.

I have to decide now to no longer upgrade, find out why it fails, or convert my laptop to Ubuntu Linux and run Windows 10 virtually.

I assume I have hardware in my older laptop that is probably no longer supported. Like firewire.

Jed Reynolds • **May 25, 2017 8:05 AM**

Some thoughts on IoT devices: wouldn't it make sense for these devices to only be able to send packets with a TTL of 1 to force them to be managed by a LAN proxy? That would at least bring in some management software that could be updated. Also, what if these IoT devices were not legally able to run a Layer 3 traffic protocol? If they only could send traffic to a mac address on a LAN or a VLAN, they couldn't participate in a DDoS. They could only be operated by an IoT management client on a LAN. Also, that would prohibit firewall emission if firewalls were prohibited from emitting IPX or whatever Layer2 protocol these devices were using. Not a perfect solution, but maybe worth considering.

Cigaes • **May 25, 2017 8:09 AM**

I think one of the key parts in securing the IoT is to move towards separation between hardware and software, which requires a certain amount of standardization of the hardware.

We were there with the PC market around 2010-2012, we could buy almost any laptop and expect any recent Linux or BSD distro to run on it with most parts supported. We are actually losing on this with some newer devices, especially hybrid tablet/netbooks: components connected with strange low-cost buses like SDIO or I2C instead of PCI, and drivers working around limitations of the hardware.

On the IoT side of the things, there are a few glimpses of that separation: alternate ROMs for home routers and wireless access points, third-party software for Canon cameras, but nothing really promising.

Of course, there is no incentive for the constructors to implement things that way, since it limits desirable features such as vendor lock-in and DRMs. But we, as consumers and voters, will need to push for that.

Werner Almesberger • May 25, 2017 8:23 AM

Regarding the problem of things not getting fixed, one approach that can yield quite acceptable results is to open (as in Open Source) orphaned platforms. If there are enough devices around for a sizable community to form, that community can often take care of things for a good while.

OpenWRT is perhaps the best-known example of an independent developer community taking care of things.

There are a few obstacles, though, among them:
1) many companies simply don't want to open any of their precious,
2) many are afraid that someone, for example a patent troll, will find something they can use against them,
3) companies may use 3rd party materials they're not allowed to release,
4) companies may be unwilling/unable to make the effort of opening a product when it's already at the end of its life.

1 and 2 are hard to address. Legislation could limit IP claims against products that have reached their end of life, but I'd imagine it to be very difficult to obtain.

3 and 4 are a question of planning: if you know from the beginning that you'll open a product in a few years, you can avoid licenses that would get in the way, keep track of any obstacles, and have a plan ready for doing this painlessly when the day comes.

Avoiding restrictive conditions imposed by 3rd parties isn't always easy, but if the industry would begin to prefer more open-friendly building blocks over restrictive ones, that should also produce a shift in what are considered standard conditions.

With open-friendly, I mean some practical goals. Some things can probably never be 100% open, due to regulatory and other reasons, but there's often good enough middle ground that provides imperfect but usable openness, e.g., modems with closed firmware but open APIs, and the bar could be raised with time.

4 could also be improved if there was some trusted 3rd party that would receive sources (and possibly updates), hold them in escrow until a set release date, and then publish them. This would a) make it possible to release future public material at the same time as product updates, which should be efficient, and b) would ensure the release will happen even if the company should go under.

The release process could be flexible. E.g., if a product should turn out to live much longer than expected, the company could just ask for postponing the release. Likewise, should they realize - before the public release - they accidently submitted something they don't want to disclose, that could be removed.

An even better approach would of course be to make firmware and such Open Source from the beginning.

An incentive for doing things this way could come from the marketing value of such an ensured opening scheme. So someone would have to come up with a pretty logo, set up the escrow entity or entities, and get it all promoted.

- Werner

Aspie+PA • May 25, 2017 8:28 AM

"We have to get it right every time, they only have to get it right once."

Sound familiar?

Were you convinced then?

Are you convinced now?

Me either.

(@{youlot} - back to the very thin of the fray, where people think & stuff is interesting.)

Andrea • May 25, 2017 8:50 AM

Asking for government intervention in such a matter is like asking help to a wild, and above all pissed off, rhinoceros to help you to fix the broken glassware...

anon • May 25, 2017 9:10 AM

Put the antennas on the outside, so they can be removed or disabled.

A lot of IOT devices with long life spans (cars, fridges, thermostats, light bulbs, utility meters) will work just fine as plain old devices without Internet access. Some of them might need to be connected once for configuration, but that's a lot different from always connected.

If devices are not connected they cannot be attacked. If they are hard wired they can be behind a firewall. If they are permanently listening for a weak broadcast no practical protection is possible.

Jim • May 25, 2017 9:11 AM

I'm not going to buy a car which is "connected" -- why would I want to be driving on the interstate at 70 MPH, knowing that someone can remotely take control of my car?

There's absolutely no need for connected cars. The perceived need for connected cars has been artificially created by people with a vested interest in being able to take control of your car.

All of the non-essential entry points (car stereo system, tire pressure monitors, etc) could be isolated from the main car network, thereby preventing someone from hacking my car. And if a software update is needed, it could be done in a much more secure way:
* Go to the dealer and let them do it manually.
* Download it and then install it manually via USB flash drive.
* Prompt the user for a password if the user chooses to allow updates "over the air".

And in all cases, there needs to be a very simple way to totally disconnect my car from all outside sources, allowing me to have complete and unhackable manual control of the car.

Bruce Schneier • May 25, 2017 9:12 AM

"Asking for government intervention in such a matter is like asking help to a wild, and above all pissed off, rhinoceros to help you to fix the broken glassware."

I disagree. Government is how society solves collective action problems. And it's our primary tool to defend ourselves against corporate power.

parabarbarian • May 25, 2017 9:27 AM

@Etienne

I feel your pain. I try to keep my few legacy Windows systems updated but that doesn't always work as well as I'd like. Consequently, I run almost all Windows installs using Oracle VirtualBox on top of CentOS 6 or 7. On all but a couple of systems, CentOS is updated nightly using yum. Kernel upgrade (requires a reboot) are done when needed.

Except for a gaming machine or AD (hack! spit!) server, I've found Windows on a VM is as good as a standalone system and can be much better protected.

ab praeceptis • May 25, 2017 9:27 AM

Bruce Schneier

Government is how society solves collective action problems.

Allow me to correct that by completing it:

Legitimate and legitimately acting government is how society solves collective action problems.

The other sentence, very slightly changed, might also be said by a large corp. ceo: -> "[gov] is our primary tool to defend our corporate power."

jdgalt • **May 25, 2017 9:29 AM**

The company that made your networked door lock may not be around anymore, but you certainly won't be the only client with that model of lock, so it may well pay some company like RedHat to write a patch for it as soon as one customer reports the problem -- and make that patch available to other customers. Today, the DMCA prevents them from doing that, so you'll be forced to throw away a perfectly good lock just as you're already forced to throw away your printer when Lexmark stops updating its drivers for each new version of Windows.

Thus, both this obsolescence issue and the resulting environmental issue should be laid at the feet of the copyright trolls who are blocking IP reform.

---

mgax • **May 25, 2017 9:36 AM**

Government can mandate that IoT devices accept 3rd party firmware and for vendors to provide documentation on writing such firmware. If the vendor fails to keep the software up-to-date, commercial or open-source solutins can step in, incentivized by market forces.

---

parabarbarian • **May 25, 2017 9:38 AM**

@Jed Reynolds

That is a darned good idea. Not perfect but restricting the IoT devices to layer 2 and using a management server to manage the IP traffic could go along way toward alleviating the problem.

@everone

One big problem with getting government involved in regulation instead of just encouraging technology development is that agencies love to load a bunch of hard-to-change regulations on top of any solution. This *will* stifle innovation and give the established corporations a serious competitive advantage over any newcomers.

Andrea • **May 25, 2017 10:02 AM**

@Bruce Schneier

"I disagree. Government is how society solves collective action problems."

I could agree with you as far as the Government is representative of the current and whole society, that is not so trivial.

"And it's our primary tool to defend ourselves against corporate power."

I would really agree with you about that, but unfortunately, tbh I can't.

Anyway, even given true all your statement and willing agree with you, because I seriously care about that, you were not able to explain how a slow bureaucracy could really cope with the issue of broken, insecure by design, technologies that are polluting the whole IoT market.

Any insecure by design thing will be really hard to secure by the most prepared and skilled people, I am looking forward to know how the secure by law could fix that...

Sorry about my weird English, but it is not my native language. (I am an EU citizen).

---

austin • **May 25, 2017 10:25 AM**

as much as i think gov't involvement is going to be necessary... i don't think that will be anything other than a quagmire or remotely effective...as much as i might want it to be

the guts of these devices are manufactured all over the world. if you want to secure the 'appliance' function you have to start at the foundation....and most of these foundation bits are made in china by nearly anonymous manufacturers who a) have no economic incentive to make their core code more complicated, b) no effective regulatory oversight to insure even minimal security is available, c) no economic incentive to either build in or modify their cmmponents for more security.

the 'mid-stream' assemblers are also all over the world and the same economic and oversight dis-incentive to spend more on making a secure device.

finally the 'marketers' who sell/resell to the 'end user' be that a commercial operation or a consumer operation have little interest in increasing the complexity of their product which would drive up their price and cost of support. the margins are too thin and will be getting thinner as many of these devices (think cameras, dvd, etc) become commoditized.

there are, to me at least, two paths.. a) wholesale rebellion by commercial and end user consumers demanding more security in these devices or b) dramatic regulatory engagement by a sovereign government.

Let's not hold our breath on a)..and move on

Option b) would require a sovereign government to prevent a risky (think all IoT) devices from being imported or sold within their borders, i.e. some sort of "security housekeeping seal of approval". That prospect is unlikely due to the sheer scope of the problem. Even if it was contemplated the scale and cost would be beyond comprehension. Even a "stick" approach has limited appeal.. who would you fine? the end user for being careless, the marketer, the assembler the component manufacturer...

I tend to be very cynical of anything useful being done to get ahead of the dramatic risks you raise. I'm of the opinion that anything IoT must not be connected to or control something that is important to me, could access personal information, could be manipulated to do harm to me or my household. If a device can't operate without the IoT function (think TV or refrigerator) and there is no way to turn it off and disable the "IoT" function...find another product.

In the meantime we will be fully entertained by the ridiculous risks being pushed at us

Austin Hutton CISA, CISM, CGEIT

Scott • May 25, 2017 10:30 AM

@Cigaes: "components connected with strange low-cost buses like SDIO or I2C instead of PCI".
I work on small embedded systems. PCI is the strange bus to me; I2C is a normal bus.

:-)

--- Scott

Terry • May 25, 2017 10:32 AM

If a vendor had written this, you would accuse them of fear mongering.

Thomas Mason • May 25, 2017 10:46 AM

The main problem that hurts people other than the ones who chose weak security, is the botnet denial of service attack problem, which can and should be solved easily by requiring ISPs to disconnect customers who have equipment participating in attacks. This could be imposed on foreign ISPs by denying them connections to the US if they don't cut off attackers. The various other problems of weak security have their effect mostly on only those who chose to purchase or maintain weak security. We have no right to take other people's freedom to chose how they will deal with their own security risk. The market should eventually work well to correct the problem as the careless become experienced with the consequences of lax security practices like using excessively complex operating systems that were not designed from the ground up for security, such as Windows or Linux.

Government regulation is very unlikely to work anyway. It doesn't appear that you can reduce good computer security to a set of best practices or safety codes. It requires great care, significant expense, deep understanding by developers, and companies that are truly serious about security. Developers working to just barely meet the best practices will not produce secure software. And shifting liability won't work either, because companies already risk their businesses by economizing on security while thinking they can get away without being compromised. They're not going to worry too much about the liability of something they think won't happen. They'll also use the cheaper tactic of insulating themselves with limited liability subsidiaries and shell companies. Most of the problem is from foreign companies that won't face liability anyway.

And what a nightmare of government regulation it would likely end up being. When the initial basic security requirements inevitably fail, it will be necessary to pile on more and more regulations in a futile attempt to reach security, until the regulations eventually become insanely complex. It's like the building and electrical codes which started out with some basic safety standards, and have morphed into volumes of arcane laws that include things like how far your bathroom counter must be away from your toilet for sufficiently comfortable elbow room.

If such laws are passed, the one critical thing is that they should automatically sunset after 5 or 10 years. Thus there would be a chance that they would go away if they are bad. But a sunset clause should not be an excuse to enact them, because once the precedent was set, they would very likely not go away, but rather just get worse.

---

de La Boetie • May 25, 2017 10:52 AM

If we put any faith in historical precedent, it's been consumer organisations and consumer advocacy that's shifted government/corporate priorities in the past - e.g. Ralph Nader and "Unsafe at any speed" for the car industry. It has emphatically NOT been governments, nor the corporates. Incidentally, I read that one of the major US car manufacturers had blocked moves to apply polarising filters to headlights and windscreens to cut out glare (and which would certainly have saved many lives over the years).

Unsafe at any speed is a good description of computers and Iot - I'm not at all reassured by the patching story on "modern" OSs, because the game just moves to social engineering and phishing. Or that the modern OSs are "terrifically weak".

One of the basic problems is that internet communications are so "invisible" in peoples' consciousness, so that obviously unacceptable things like mass surveillance without warrant are accepted because the harm is not so obvious, nor is the offence.

Bruce's advocacy helps of course, but I think it will take some more well-publicised disasters with loss of life to tilt things to a point where the ridiculous government/IC story of attack and weakness starts to shift the other way.

Jordan • **May 25, 2017 10:57 AM**

Some good news(?): if the device is driven through a cloud service, as many are, it automatically turns into a paperweight when the vendor goes out of business.

My first-order rule for IOT security is "no remote inbound connections". Don't punch holes in my firewall! If the device's remote features operate by having it connect out to the vendor's servers, it's much harder for the bad guys to attack it. (Alas, that still won't stop major players who can infiltrate the vendors.)

Andrew • **May 25, 2017 11:04 AM**

Another unfortunate aspect of government regulation is that legislation works on a timescale of years and decades, but technology works on a timescale of weeks and months. Rules tend to get written as point solutions that specify a particular technology rather than the desired outcome. An excellent example is the current crop of laws that restrict texting while driving. While an excellent idea (to reduce distracted driving), they specified **texting**. What about email? Tweeting? Instagram? Snapchat? Saving a text memo? Or whatever new app comes out tomorrow.

I can't help but think most government regulations would try to micromanage specific solutions. No open SSH or telnet is good, but what about SQL injection? How do we avoid this? The concept of a UL-type system has some merit.

Andrea • **May 25, 2017 12:04 PM**

@Jordan

"if the device is driven through a cloud service, as many are, it automatically turns into a paperweight when the vendor goes out of business"

Actually, in such a case, when the vendor goes out of business is just making the device more vulnerable, it will be alot easier for any fake cloud service to take control over the device.
I expect that a lot of unaware people, I am pretty confident that I haven't to remind you that mostly IoT customers are not IT security people, will be pleased that these devices will be running round and smooth even if the vendor has gone out of business...

---

albert • **May 25, 2017 12:08 PM**

Barring meaningful government regulation (unlikely),

I would ask that warning labels be required on all IoT systems, stating the risks, and the liability assumed by the user (all), and the vendor (none).

Simple and cheap.
. .. . .. --- ....

Andrea • **May 25, 2017 12:31 PM**

@albert

"would ask that warning labels be required on all IoT systems, stating the risks, and the liability assumed by the user (all), and the vendor (none)."

I am pretty confident that you are aware that using smartphones without vocal commands and text readers meanwhile driving is a sanctioned behavior in most modern Western democracies, other than, and above all, a dangerous driving style, nevertheless I see every day alot of people doing it carelessly.

Let me have some doubt that a warning label could help to fix the issue.

Maybe we need a cultural revolution, making the people less careless and more attentive and careful to their whole life, also the digital and online one, otherwise I am pretty confident that this time is IoT and its insecure by design, next time it will be something other still insecure by design that will be expose people to any sort of risk and threat...

...But given the current world, has this cultural revolution any chance to even get started? Maybe, in such a case, any Government help to improve people awareness could be helpful, but please not enforcing security by law, we need people aware, not people sanctioned...

Duty to warn • May 25, 2017 1:44 PM

If you notice the comments on influential blogs and sites, there will be folks who will troll supporting pro-business views without meeting their burden of persuasion that those viewpoints are best solution for social problems eg net neutrality or problem posed by insecure IOTs.

Some of these commentators are dogmatic that they won't reveal the basis of their extremest views; premises and rationality are missing.

Some commentators are there just confuse by making fallacious and unsupported arguments and spreading outright lies.

No one one person has the cognitive resources to unravel the complex deceptive brain-washing by these paid and unpaid trolls who can go anonymously without disclosing their affiliations and that they are paid to pollute the discourse and over-burden genuine and good faith explorations of important social problems that require collective input and discussions in order to arrive at solutions that are not biased at some self-serving groups like US chamber for commerce or billionaires.

---

albert • May 25, 2017 2:41 PM

@Andrea,

-Of course- it's not going to 'fix the issue', but it's a compromise between regulation and consumer protection. Manufacturers will fight -any- sort of regulation tooth and claw. Warning labels would be a major victory on the side of sanity; no mean feat in todays world.

Let's start with crawling, then we can try walking later..

. .. . .. --- ....

---

neill • May 25, 2017 2:43 PM

the networks are the key component here
block unwanted traffic, then nothing will be able to spread - or only very limited

i repeat myself, too:

we CAN have outdated, insecure devices, and happily use those, IF our 'bubble' is protected by either our network, or our ISPs.
i'll happily give my ISP the authority to filter my traffic IF that keeps me safe and saves $ for me not setting up my own filters.
they know anyways what i do online.

IoT manufacturers will never pay for security nor updates, since the end user is most likely to pick the cheapest device that does the job. since most devices come nowadays from asian countries you won't be able to collect $ for damages anyways.

hence WE have to protect ourselves, with smart networks.

i don't even want passwords for my cameras, i don't need folks bothering me asking for those, when they want to view the cams.
those need to be viewed from two or three 'outside' IPs, but other than that, there's NO need for my cams trying to connect to anything else.

same for my (yet to be bought) smart fridge. it may want to inquire at 2 or 3 local frequently visited groceries to find the best deal on milk if need would be, but again, no need to connect to anything out-of-state or abroad.

Clive Robinson • May 25, 2017 2:56 PM

@ parabarbarian, Jed Reynolds

> That is a darned good idea.

Sadly I don't think it will happen, because the IoT companies have way to much invested in the data exfiltration for profit game. Where users data provides the profit...

But if a certain major credit rating organisation is correct Google has run out of steam thus profit in the selling of "user meta data". If they are correct it may well mean that the bubble is bursting on the big data scam (for that is surely what it is).

If so, then that may well kill the data exfiltration for profit game that is underpinning parts of the IoT market, and thus pull it down, or burst the bubble entirely as often happens with new tech sectors as history shows from Victorian times onwards.

Fred • May 25, 2017 3:15 PM

For home users, the biggest design problem with IoT devices (aside from the lack of updates) is that, by default, many of them expose themselves to the internet by using uPnP to tell the consumer router/firewall that they are hosting internet services. Mirai would have had very few victims if that hadn't been the case.

Pedro Fortuna • May 25, 2017 4:55 PM

On way or the other, Reverse Engineering is going to be a very profitable activity :-)
Bad guys reverse engineer to find security flaws they can exploit.
Good guys reverse engineer code to be able to put out patches for products made by companies that are no longer there.

Maybe legislators can force closed source products to use Code Escrow services. In the case of bankruptcy, that code could be somehow given to the good guys. Putting that code in open source could be another option, but not before checking it for obvious flaws that could be low hanging fruit for the bad guys.

Lawrence D'Oliveiro • May 25, 2017 6:32 PM

Yes, there is one bit of regulation that can force companies to maintain old products: tell them that, as long as they claim "intellectual" property rights over those products, then they must accept property responsibilities as well. If your property is causing a nuisance to others, then the onus is on you to fix it, not on anybody else.

Currently, I believe, the US copyright term is 90 years. So Microsoft, for example, should continue to support Windows XP for, what is it, another 74 years? After all, they were always quite clear that they never "sold" it to you, only "licensed" it. So as long as they own it, they have to look after it.

Clive Robinson • May 25, 2017 7:08 PM

@ Pedro,

> Maybe legislators can force closed source products to use Code Escrow services. In the case of bankruptcy, that code could be somehow given to the good guys.

There is a problem with the "good guys" notion which is similar to the "Defense Spending" conundrum.

Let me put it this way,

> You are not a murderer untill you kill someone, but killing someone is not sufficient to make you a murderer in the eyes of both society and the law.

That is the definition of good or bad is at best difficult and context sensitive.

Many people in the US consider their nation to be "The Good Guys" whilst atleast as many if not a lot more outside the US consider the US to be "The Bad Guys". As someone once noted about revolutions and other civil unrest, "Those looking out over the barricade consider themselves to be in the right, and those outside in the wrong, whilst those looking in likewise consider themselves to be in the right and those inside to be in the wrong". Wars are based on such illogical and contradictory moral perspectives.

Thus the least thing you can say is "One man's good guy is another man's bad guy", but you also have to realise that "good guys go bad" thus they have to be watched, but this raises the problem of "Who watches the watchers" which is one of those "lesser fleas" or "turtles all the way down" problems. Which unfortunatly is why human nature tends not to the "majority view point" but to the "Might is right" and hence war and destruction.

---

anon • May 25, 2017 7:39 PM

@Thomas Mason • May 25, 2017 10:46 AM

> The main problem that hurts people other than the ones who chose weak security, is the botnet denial of service attack problem

Alas, that may not be true. The IOT includes *Things*. How many million refrigerator compressors can be cycled with millisecond precision without major blackouts or destroying parts of the grid?

Maurice Volaski • May 25, 2017 10:12 PM

"Most people have set up their computers and phones to automatically apply these patches, and the whole thing works seamlessly."

Seamlessly?

http://www.infoworld.com/article/2889295/microsoft-windows/20-epic-microsoft-windows-auto-update-meltdowns.html

Pedro Fortuna • May 26, 2017 3:51 AM

@Clive
Yes, I do realize telling who are the "good guys" is extremely tricky, to say the least. Even the gov engages in mass surveillance activities, using undisclosed vulnerabilities as cyber weapons, and thus becoming the "bad guys" in the eyes of many people.

Another model could be, as part of the code escrow service, companies would have to specify either a security company or a panel of security practitioners they trust, external to the company, that would have access to the code in the case of bankruptcy, and that would become responsible for the security of that code. They would be liable if it is determined that no efforts were done to audit the security of the code after the bankruptcy. Obviously, they would need to get paid for assuming that responsibility.

Dan H • May 26, 2017 7:01 AM

@Clive

You and the rest of Europe don't speak German today because the US - twice - had to fight to keep you free. While the US was fighting in Europe in WWII, there was also a war in the Pacific that was primarily fought only by the US with some help from Canada, the UK, Australia. But the contribution of those countries wasn't near the help Europe received twice from the US.

Also, if the US is the "bad guy," then why is the United States the top country for receiving migrants? When do you hear someone saying they want to migrate to Mexico, China, Guinea, Peru, Syria, Guatemala, Panama, Cambodia, etc.? According to the UN, France, the UK, among others, promoted policies to lower immigration into their countries.

Where did Albert Einstein, who was born in Germany, migrate? To the bad guy, the United States.

The best security for IoT is to realize the refrigerator and garage door opener don't have a need to be connected.

Robin • May 26, 2017 7:54 AM

@DanH:

"*The best security for IoT is to realize the refrigerator and garage door opener don't have a need to be connected.*" That I can agree with, at least as a first approximation.

Unfortunately the rest of your post pretty much makes @Clive's point:

"*Many people in the US consider their nation to be "The Good Guys" whilst atleast as many if not a lot more outside the US consider the US to be "The Bad Guys".*"

The USA eventually came in on the side of the allies in both World Wars, but arguably it was the USSR which drained the resources of the German Army in WW2 which turned the tide, which you do not mention *at all*.

But heck, this is ancient history.

As for people migrating to the US that is no sort of an argument; people will swear allegiance to a mafia boss if that seems a sensible course of action.

The Less Changes The More Secure • May 26, 2017 7:55 AM

Almost all of the software updates are really just changes. Take Windows which goes round-n-round back to similar designs it had years ago.
The churning is really for data-mining to monetize the product (people).

True technology changes are MUCH slower. For example Intel has stalled-out and STILL not provided 4K display support.

This is why I use the Linux kernel/operating system. They focus is on making technology improvements to support new hardware and security features.
In contrast the Windows updates rarely benefit customers.

If MS quit making so many worthless changes, Windows security would improve dramatically.
This week we learn MS does not respect the privacy settings even in the Enterprise Edition. Or Google not respecting student privacy. The cycles continue to worsen as the hand-fed addicts continue to propel stock prices.

The two most popular technologies are proprietary phones and Windows. Both keep their customers captive and vulnerable.
One frequently should issue security updates but instead pushes the customer into purchase new hardware.
The others thrashing creates new vulnerabilities to force customers to submit to even more intrusive data-mining. Customers cannot pick just the security patches or even know what they contain.

Now our whole economy is dependent upon these wickedly flawed corporate shareholder-value cycles. The terrorists are NOT being stopped either. Instead the secret data-mining is used for the next promotion or as a political weapon.

My guiding principle is the less code changes, the more secure it can be made.

My guiding strategy is to obscure my computer hardware, operation system and location by feeding random user agent strings from a locked-down browser. Its very effective hiding behind a VPN DD-WRT double firewall router.

Subscribe to comments on this entry

Leave a comment

Login

Name (required):

E-mail Address:

URL:

□ **Remember personal info?**

Fill in the blank: the name of this blog is Schneier on __________ (required):

Comments:

Allowed HTML: <a href="URL"> • <em> <cite> <i> • <strong> <b> • <sub> <sup> • <ul> <ol> <li> • <blockquote> <pre>

Preview **Submit**

← Hacking Fingerprint Readers with Master Prints

Security and Human Behavior (SHB 2017) →

Schneier on Security is a personal website. Opinions expressed are not necessarily those of IBM Resilient.